Using Compact DNSSEC and Self-signed Certificate to Improve Security and Privacy for Second-Level Domain Resolution

Lanlan Pan (潘蓝兰)

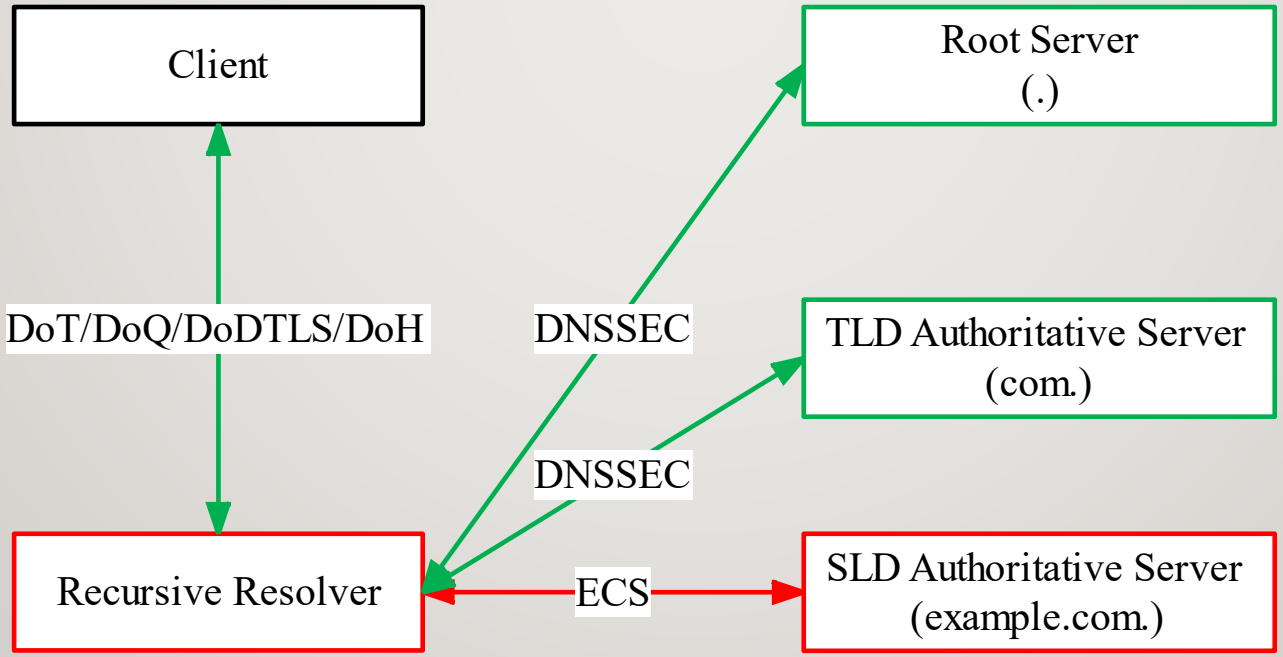
abbypan@gmail.com

Outline

- Introduction
- Challenges
- Our Scheme
- Conclusion

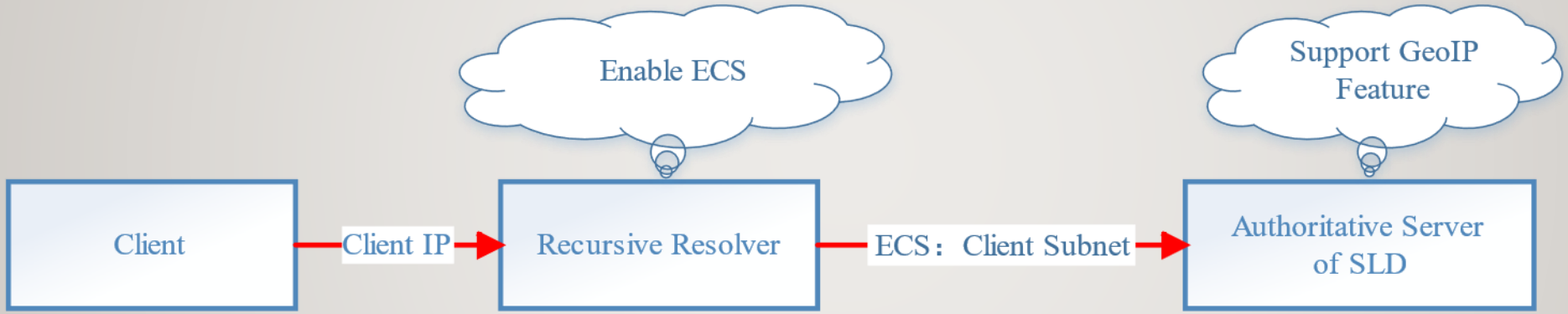
Introduction

- DNS's plaintext traffic makes it vulnerable to domain hijack attacks and user privacy leakage.
- DNSSEC is to defend against the domain hijack attack.
- DoT/DoQ/DoDTLS/DoH are deployed on some recursive resolvers to protect user privacy.
- However, there are still some challenges to the second-level domains (SLD) resolution between recursive resolver and SLD authoritative server.



Challenges: ECS Privacy Leakage

- ECS extension raises privacy concerns since the recursive resolver leaks client subnet information on the resolution path to the authoritative server of SLD.



Challenges: DNSSEC Low Deployment on SLD.

- The main design of DNSSEC is cryptographic and technical complex.
- ICANN shows that there are only 4% SLDs in the 'com' zone deployed DNSSEC until October 2024.

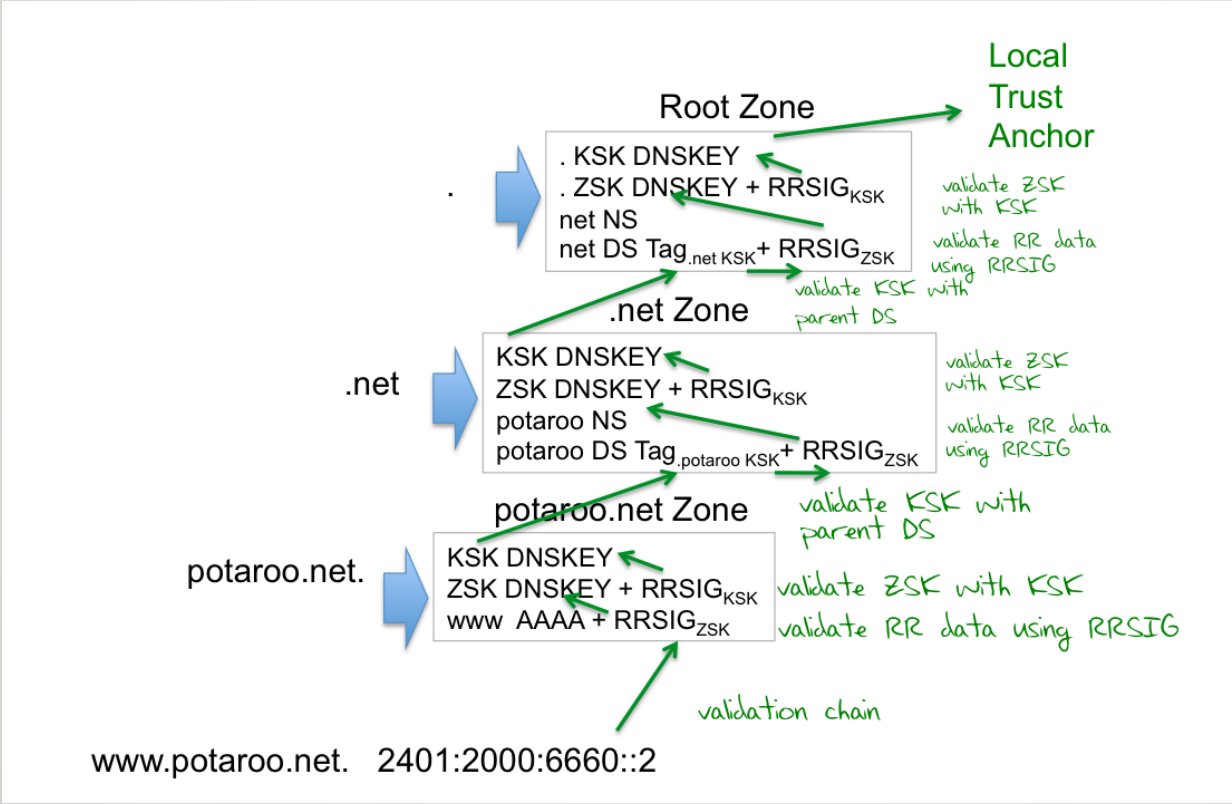


Figure is from : https://www.potaroo.net/ispcol/2010-06/dnssec.html

Challenges: DDoS Risk

- DNS random subdomain attacks and amplification attacks are commonly used distributed denial-of-service (DDoS) attacks.
- As analyzed by Nexusguard, the DDoS amplification power of the authoritative server of SLD could be surged to more than 45X after deploying DNSSEC.

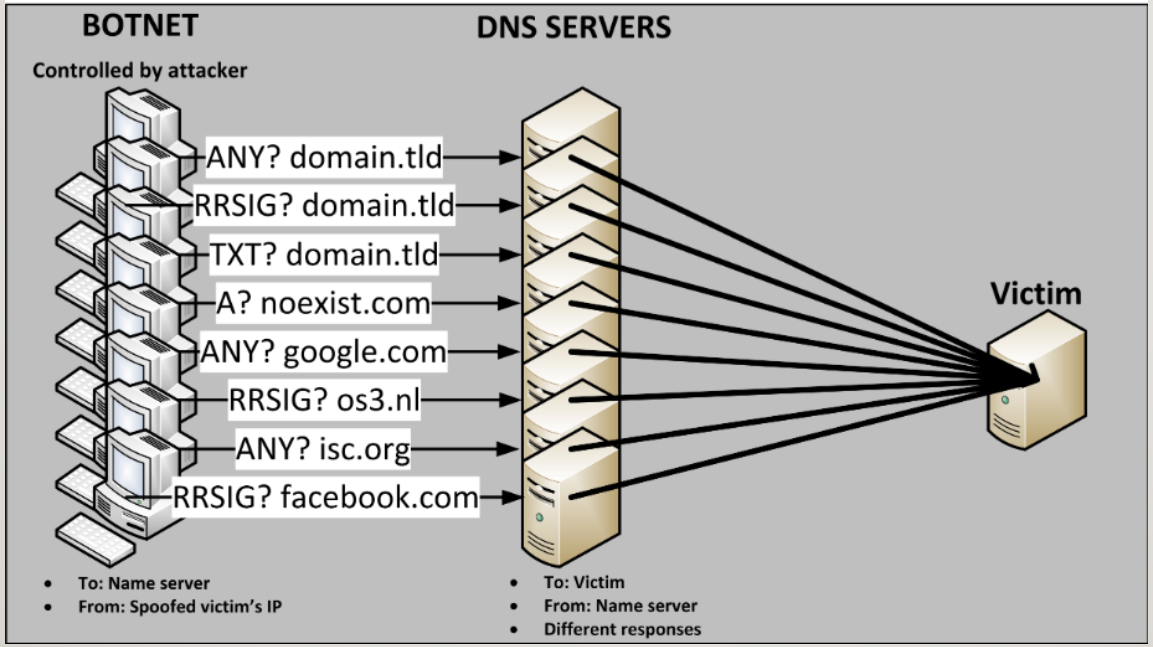
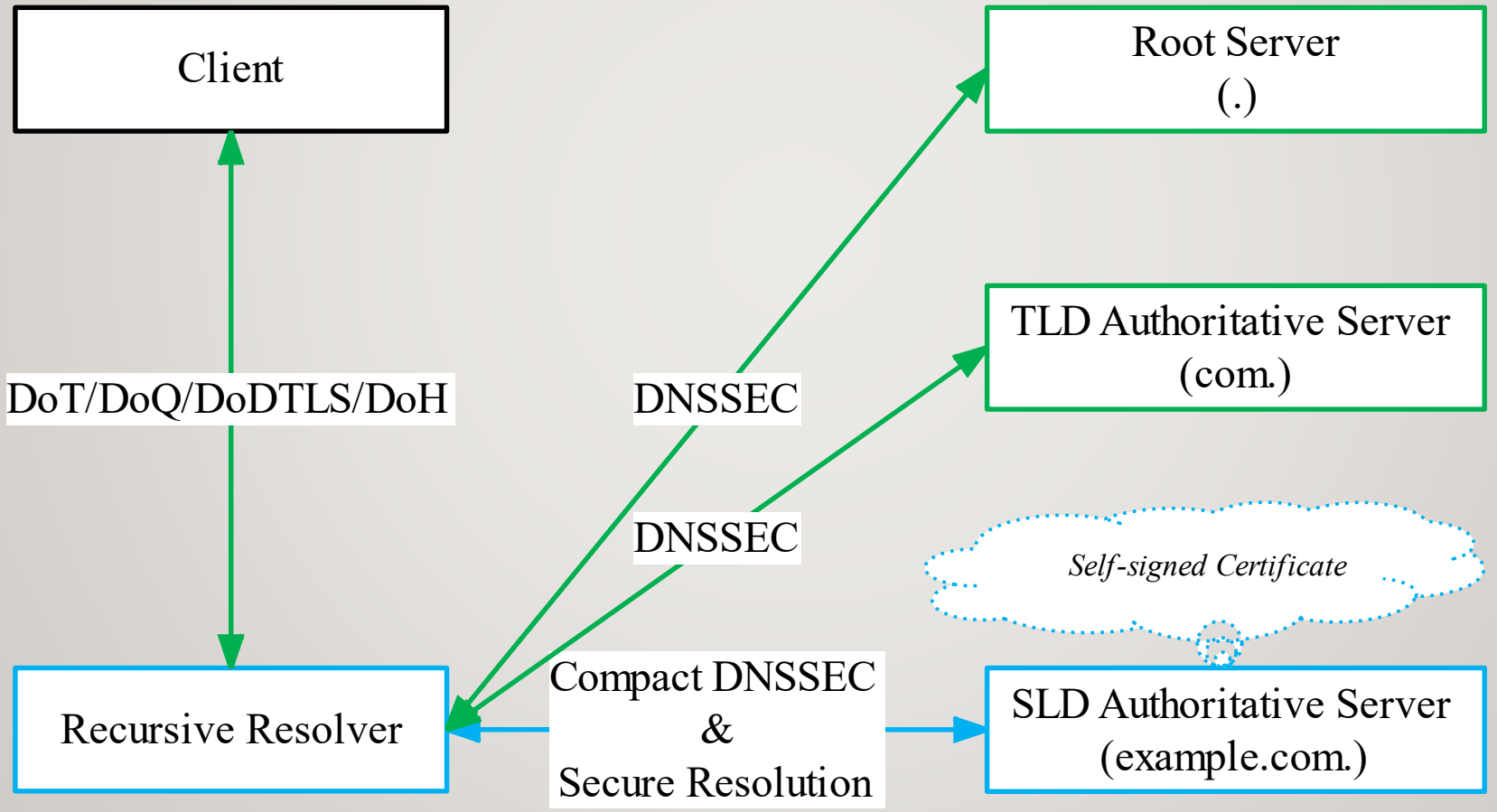


Figure is from : https://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf

Our Scheme

- We describe a scheme with compact DNSSEC and self-signed certificate to improve security and privacy for SLD.



Our Scheme

- We describe a compact DNSSEC scheme.
  - It is specifically targeting the NS/A/AAAA/TLSA resource record sets (RRsets) associated with NS resource record (RR), aimed to ease the operation burden of DNSSEC deployment and reduce the DDoS amplification power.
- The authoritative server of SLD is to provide the secure resolution service with a self-signed certificate, and publish a domain-based authentication of named entities (DANE) TLSA reord for the self-signed certificate information.
- The recursive resolver is to verify the RRSIG records provided by the compact DNSSEC and make secure resolution through the DoT/DoQ/DoDTLS channel to mitigate the ECS privacy leakage.

Authoritative Server: Provide Secure Resolution Service with Self-signed Certificate for SLD

- The NS records should be written into the subjectAltName extension field of the self-signed certificate.
- The two NS servers (‘ns1.example.com’ and ‘ns2.example.com’) can provide secure resolution services on port 853 with the self-signed certificate.
- RFC9539 discussed more operation details.

Authoritative Server: Publish the TLSA records

- Define the well-known subdomains (‘ 853. tcp’ and ‘ 853. udp’) for each NS record to publish its certificate information and configure the corresponding TLSA records.
- The TLSA record indicates the digest of the subject public key of certificate.
- The ‘ 853. tcp’ subdomain is for DoT service run on TCP port 853, and the ‘ 853. udp’ subdomain is for DoQ/DoDTLS service run on UDPport 853.

Table 1: The NS/A/AAAA/TLSA Records Associated With NS

example.com.	345600	IN	NS	ns1.example.com.
example.com.	345600	IN	NS	ns2.example.com.
ns1.example.com.	345600	IN	A	11.22.33.44
ns1.example.com.	345600	IN	AAAA	::11.22.33.44
ns2.example.com.	345600	IN	A	55.66.77.88
ns2.example.com.	345600	IN	AAAA	::55.66.77.88
_853._tcp.ns1.example.com.	3600	IN	TLSA	(3 1 1 63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364)
_853._udp.ns1.example.com.	3600	IN	TLSA	(3 1 1 63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364)
_853._tcp.ns2.example.com.	3600	IN	TLSA	(3 1 1 63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364)
_853._udp.ns2.example.com.	3600	IN	TLSA	(3 1 1 63cbfcafa3284cc46b1676a99dbc09d8acadf9050cf876de79ac1e5776bbd364)

Authoritative Server: Configure Compact DNSSEC

Configure compact DNSSEC for ‘example.com’ to cover the critical records:

① the delegation signer (DS) record

② the DNSKEY records

③ the NS/A/AAAA/TLSA records associated with NS

Recursive Resolver: Gain trustworthy records associated with the NS of SLD

① Verify the DS RRSIGs and DNSKEY RRISGs following the DNSSEC chain.

② Verify the RRSIGs associated with the NS of SLD.

③ Cache the trustworthy records of the SLD ‘example.com’, following DNS TTL configuration.

Recursive Resolver: Make Secure SLD Resolution

① Receive some subdomain queries of example.com from the client.

② Make a TLS connection with the secure resolution service of the authoritative server, check if the hash of the subject public key of the received certificate matches the TLSA record of the NS, build up the secure DoT/DoQ/DoDTLS channel.

③ Make DNS resolution through the secure channel, ensure that the DNS responses are trustworthy.

④ Return the trustworthy DNS responses to the client.

Compact DNSSEC Consideration

- With full zone DNSSEC, the amount of RRSIGs increases linearly O(n) with the subdomains.
- Our compact DNSSEC has constant RRSIGs O(1).

Table 2: RRSIG Amount Comparison

Scheme	Signed RRsets Scope	Amount of RRSIGs
Plaintext DNS	None	0
Full Zone DNSSEC	All records of all subdomains	$O(n)$
Compact DNSSEC	The NS/A/AAAA/TLSA records associated with NS	$O(1)$

Self-signed Certificate Consideration

- Recursive Resolver fully trusts all widely known CAs, which makes it vulnerable to certificate hijacking attacks.
- Compared to the PKI-based certificate, the self-signed certificate is lightweight and following the pure DNSSEC trust chain to avoid the domain hijacking.

Scheme	Issuer	Configure TLSA Record and RRSIG	trust chain
Self-signed	AS_{sld}	Must	DNSSEC
PKI-based	widely known CA	Optional	widely known CA

Secure SLD Resolution Consideration

- Recursive resolver can make a secure resolution with the authoritative server to deal with the ECS privacy leakage issue.
- The secure DoT/DoQ/DoDTLS resolution channel can also protect them from domain hijack attacks through trustworthy TLS authentication.

Scheme Comparison

- Our scheme makes encrypted resolution between RS and AS_{sld}, which can defend against the passive monitoring of the client subnet information and mitigate the ECS privacy leakage problem.
- Compared with the full zone DNSSEC, our compact DNSSEC scheme only calculate RRSIG on the records associated with NS, which can limit the amplification power of AS_{sld}.
- Our compact DNSSEC scheme is focused on the records associated with NS, which can significantly reduce the operation burden of DNSSEC deployment.

Table 4: Scheme Comparison

Scheme	DNSSEC	Authenticated NXDOMAIN Response	Prevent Zone Enumeration	Encrypted Resolution Path	Secure Resoultion Service	DNS Amplification DDoS Attack
Plaintext DNS (Mockapetris, 1987)	×	×	×	×	×	×
DNSSEC with NSEC (Schlyter, 2004)	Full Zone	√	Weak	×	×	√
DNSSEC with NSEC3 (Laurie et al.,)	Full Zone	√	√	×	×	√
Murakami T., et al (Murakami et al., 2023)	×	×	×	$Client \leftrightarrows AS_{sld}$	DoT	×
Gillmor D., et al (Gillmor et al., 2024)	×	×	×	$RS \leftrightarrows AS_{sld}$	DoT/DoQ	×
Sunahara S., et al (Sunahara et al., 2022)	×	×	×	$Client \leftrightarrows RS \leftrightarrows AS_{sld}$	DoH	×
Our Scheme	Compact	×	×	$RS \leftrightarrows AS_{sld}$	DoT/DoQ/DoDTLS	×

Evaluation: Zone File Size

- Our compact DNSSEC scheme is approximate with plaintext DNS with constant RRSIGs: O(1).

Table 5: Zone File Size (Bytes)

Schemes	**Number of Existing Subdomains (N)**			
N	**100**	**1000**	**10000**	**50000**
Plaintext DNS	4085	33554	330143	1648649
DNSSEC with NSEC	52275	494113	4912291	24549305
DNSSEC with NSEC3	79185	596264	5734853	28573360
Our Scheme (DoT)	5273	34741	331331	1649811

Evaluation: Average Resolution Time

- Our scheme makes a single keep-alive DoT connection for all subdomains but does not create a unique DoT connection for each subdomain.
- Therefore, our scheme gains the minimum resolution time of the four schemes in the evaluation when N≥1000.

Table 6: Average Resolution Time (Milliseconds): Existing Subdomains

Schemes	**Number of Existing Subdomains (N)**			
N	**100**	**1000**	**10000**	**50000**
Plaintext DNS	0.027	0.023	0.023	0.028
DNSSEC with NSEC	0.025	0.024	0.024	0.026
DNSSEC with NSEC3	0.026	0.023	0.023	0.027
Our Scheme (DoT)	0.032	0.013	0.010	0.010

Table 7: Average Resolution Time (Milliseconds): Random Non-existent Subdomains ($M = 50000$)

Schemes	**Number of Existing Subdomains (N)**			
N	**100**	**1000**	**10000**	**50000**
Plaintext DNS	0.026	0.028	0.028	0.027
DNSSEC with NSEC	0.023	0.024	0.024	0.024
DNSSEC with NSEC3	0.024	0.023	0.023	0.023
Our Scheme (DoT)	0.009	0.009	0.010	0.010

Evaluation: Average Payload Size (Existing subdomains)

- The DDoS amplification factor of plaintext DNS is about1.31; DNSSEC with NSEC/NSEC3 is about 3; our scheme is about1.21.
- Our scheme has the minimum DDoS amplification factor of the four schemes since it makes a single keep-alive DoT connection.

Table 8: Average Request Payload Size (Bytes): Existing Subdomains

Schemes	**Number of Existing Subdomains (*N*)**			
N	**100**	**1000**	**10000**	**50000**
Plaintext DNS	51.16	50.99	50.96	50.96
DNSSEC with NSEC	62.16	61.99	61.96	61.96
DNSSEC with NSEC3	62.16	61.99	61.96	61.96
Our Scheme (DoT)	76.95	73.36	73.00	72.97

Table 9: Average Response Payload Size (Bytes): Existing Subdomains

Schemes	**Number of Existing Subdomains (*N*)**			
N	**100**	**1000**	**10000**	**50000**
Plaintext DNS	67.16	66.99	66.96	66.96
DNSSEC with NSEC	185.16	184.99	184.96	184.96
DNSSEC with NSEC3	185.16	184.99	184.96	184.96
Our Scheme (DoT)	103.01	88.57	87.12	86.99

Evaluation: Average Payload Size, Non-existent subdomains(M=50000)

- The DDoS amplification factor of plaintext DNS is about 1.82; DNSSEC with NSEC is about 8.44; DNSSEC with NSEC3 is about 12.10; our scheme is about 1.56.
- The DDoS amplification factor of our scheme is approximate with plaintext DNS, lower than 2.
- DNSSEC with NSEC/NSEC3 have high amplification factors since they include RRSIG and NSEC/NSEC3 records in the response payloads.

Table 10: Average Payload Size (Bytes): Random Non-existent Subdomains ($M = 50000$)

Schemes	**Request Payload Size**	**Response Payload Size**
Plaintext DNS	54.96	99.96
DNSSEC with NSEC	65.96	556.46
DNSSEC with NSEC3	65.96	798.29
Our Scheme (DoT)	76.97	119.99

Conclusion

- Our Work
  - We propose a secure resolution scheme for SLD.
  - Our scheme requires a self-signed certificate to run the secure resolution service and make a compact DNSSEC configuration.
  - We focus on making the recursive resolver gain the trustworthy authoritative server addresses of SLD, set up a secure resolution channel by TLS, and finally defend against domain hijack and privacy leakage.
- Limitation
  - We don't create a new DNS extension but focus on enhancing the trustworthiness validation of the NS and privacy protection.
  - We setup the secure channel based on the standardized DoT/DoQ/DoDTLS, and don't discuss about other alternative solution such as DNSCurve.
  - Our compact DNSSEC scheme does not cover the entire zone and does not deploy NSEC/NSEC3 to mitigate DNS random subdomain attacks.
- Future Work
  - Do more impact evaluation on our scheme and deploy it on the DNS system.

THANK YOU

Q&A